SaaS Lawyer Kristie Prinz Presents on “Best Practices for Drafting SaaS Contracts that Reduce the Sales Cycle”

SaaS Lawyer Kristie Prinz presents on “Best Practices for Drafting SaaS Contracts that Reduce the Sales Cycle” in March 2017. A copy of the video recording is available for viewing at this link: https://theprinzlawoffice.vhx.tv/products/draft-saas-contract-to-reduce-customer-sales-cycle

---

SaaS Contract Lawyer Kristie Prinz to Speak on “Best Practices for Drafting SaaS Contracts that Reduce the Customer Sales Cycle & Avoid Disputes”

Silicon Valley attorney Kristie Prinz will be speaking on “Best Practices for Drafting SaaS Contracts that Reduce the Customer Sales Cycle & Avoid Disputes” at a webinar hosted by The Prinz Law Office on March 24, 2017 at 10 a.m. to 11:30 a.m. PST. To sign up for the event, please register at the following

link: http://prinzlawstore.com/saas-customer-agreements/.

Service Level Agreements: What is a Service Level Agreement or “SLA” and When Do You Need One?

If you are in the software industry, you probably have heard of a “service level agreement” or “SLA” but do you really understand what a service level agreement is or why you might need one? The Silicon Valley Software Law Blog addresses this issue in the following blogpost:

http://www.siliconvalleysoftwarelaw.com/service-level-agreements-what-is-a-service-level-agreement-or-sla-and-when-do-you-need-one/

Recent Class Actions Provide Valuable Lesson on Why SaaS Contracts Should Be Drafted to Fit A Company’s Business

Model

If your company is like most, you may be using a software agreement that has nothing to do with your company's business practices or business model. Why is this a bad idea? Well, several recent class action suits provide a recent example of why this can be very problematic for a software company. The Silicon Valley Software Law Blog addresses this issue in the following blogpost:

http://www.siliconvalleysoftwarelaw.com/recent-software-class-actions-provide-valuable-lesson-on-why-saas-contracts-should-be-drafted-to-fit-companys-business-model/

Recent Software Class Actions Provide Valuable Lessons

When SaaS companies and start-ups first contact me, they are often doing so with the idea that there are a few really well SaaS template contracts circulating in the SaaS industry and they seeking the" right" attorney to provide that industry-standard template to them. Alternatively, they contact me telling me that they've already put together a draft SaaS contract, and that they just want me to look over and "bless" what they've already written based on a particular SaaS company's contract available for download on the Internet.

In these cases, which are the norm rather than the exception, I often encounter significant push-back when I first suggest to them that they are approaching the SaaS contract drafting process entirely the wrong way. I always explain that a well-drafted SaaS contract should be tailored to their specific

business model, and then I proceed to ask them a number of questions about their business model, which they generally aren't prepared to answer. They often then proceed to get frustrated by all the questions about their business, when all they are actually looking for is the "right" contract template.

If you are in the SaaS industry and have created your customer contract in a similar fashion, or committed the other common software contracting "sin" of caving into pressure exerted by a potential customer and just agreed to their standard agreement terms because you wanted to close a deal with them, then you may want to consider the example of recent litigation against an industry leader, which adopted contract language which was then alleged not to match the company's business practices.

The litigation at issue involves class action suits against the McAfee brand security software: **Williamson v. McAfee, Inc.,** No. 5:14cv00158 (N.D. Cal. Aug. 30, 2016) and **Kirby v. McAfee, Inc**., No. 5:14cv02475 (N.D. Cal. May 29, 2014). Both cases focus on the company's business practices surrounding its use of automatic renewal clauses—a standard practice widely adopted throughout the SaaS industry. The litigation is ongoing: while the court granted final approval of a **settlement** in both cases, an appeal has been filed. (See **posted notice**).

The particular contract clause at issue in the Williamson case is a common clause routinely included in SaaS contracts that stated at autorenewal customers would be charged the "then-current" price for the product. However, the Williamson complaint alleged that the actual practice of the company was to charge customers upon autorenewal a higher price for the product than the price that the customer could have purchased the product for elsewhere.

The particular contract clauses at issue in the Kirby case

stated that customer would be automatically enrolled in the autorenewal program and that a customer's credit or debit card could be charged at autorenewal even after it had expired. The Kirby complaint alleged that the actual practice of the company was to import into its billing system updated customer credit or debit card information provided by Visa or MasterCard rather than procuring a new authorization from client when the prior authorization became invalid, and to charge the customer at autorenewal at a higher price than originally paid without the customer's express consent.

While there are a number of allegations made against McAfee in these class action suits, a fundamental problem alleged was that the terms of service binding the customer did not match the company's actual business practices, and that the customer did not provide consent to the company's actual autorenewal practices.

While these particular suits were filed against McAfee, the business practices alleged in these cases are perhaps the current standard of conduct for today's software industry. Furthermore, I would argue that more often than not terms of service are adopted by companies without any consideration whatsoever of the actual technology and business model for the software or SaaS product, so it is probably rare for the terms of service to match the company's actual business practices. Thus, it is my assertion that these cases provide an excellent primer of the risks of adopting terms of service that do not match the actual practices of the business. It's still not clear what the ultimate price tag on this matter will reach on the part of the company, but it's clear it will be multiple millions of dollars in costs and expenses.

Moreover, these cases demonstrate the importance of consent to having an effective autorenewal clause. State laws applicable to these cases did require the procurement of clear and conspicuous consent to autorenewal, which McAfee is alleged not to have had in these particular sets of facts. Obviously,

any deficiency with consent could have easily been addressed through the adoption of better business practices and terms that would demonstrate clear customer consent in compliance with applicable state laws.

The bottom line is that terms of service should not be adopted by a SaaS company without a thorough consideration of the technology, the business model, and the business practices of the company. Even common business concepts like autorenewal accepted across the board within the industry may lead to costly lawsuits if insufficient consideration of business practices is contemplated in conjunction with the drafting of terms of service.

FTC Enforcement Actions Should Provide Warning to Software Industry about Privacy

If your software company is like most, you have probably spent little or no time contemplating what needs to be in your company's privacy policy. In fact, what your company is currently calling its privacy policy was likely copied from a third party website years ago and never given much thought since. Meanwhile, your company is likely collecting and aggregating user data and looking for new opportunities to monetize it. Sound familiar?

Well, if this is your company's situation, you may want to

rethink how you are operating in light of recent enforcement action by the FTC on corporate data collection practices.

On February 6, 2017, the FTC announced that VIZIO, Inc. had agreed to pay $2.2 million to settle charges by the FTC and Office of the New Jersey Attorney General that it installed software on its TVs to collect data regarding consumer viewing without their knowledge or consent. In its **complaint against VIZIO**, the FTC alleged that VIZIO had manufactured televisions that continuously tracked consumer viewing on the television and transmitted this information back to VIZIO, and also had remotely installed the same proprietary software on previously sold televisions. In addition to collecting information about consumer viewing, the **FTC alleged in its complaint** that the software had collected information about the television, IP address, wired and wireless MAC addresses, WiFi signal strength, and nearby WiFi access points. The **FTC further alleged in its complaint** that VIZIO had then entered into third party contracts to sell the data collected to third parties for the purpose of measuring the audience, analyzing advertising effectiveness, and targeting advertising to particular consumers. While VIZIO's contracts had provided only aggregate data to the third parties, those contracts did provide segmented demographic information by sex, age, income marital status, household size, education, home information, and household value. According to the **FTC Complaint,** VIZIO did make a privacy policy available on its website, but the only onscreen notifications provided to consumers were vague and timed out after 30 seconds, never sufficiently informing consumers as to VIZIO's data collection practices with the software installed on their televisions. **The FTC alleged** that VIZIO's actions in deceptively omitting material facts constituted deceptive acts or unfair practices prohibited by Section 5(a) of the FTC Act.

In the **stipulated order**, VIZIO was ordered to take all the following actions before collecting any further data from

consumers:

- Prominently disclose to consumers **"separate and apart"** from the privacy policy specifics on the data to be collected, what would be shared with third parties, the categories of third parties who would receive the data, and the purpose for which the third parties would receive the data.
- Obtain affirmative express consent from consumers at the time of disclosure and upon any material changes.
- Provide instructions at the time of obtaining consent to how consumers may revoke consent.

The **stipulated order** then gave specific guidelines on what would constitute "prominent" disclosure

The **stipulated order** also required the destruction of the previously collected data, the mandated creation of an internal privacy program meeting certain requirements, and third party oversight going forward regarding the privacy controls in place at the company.

Clearly, the FTC intended to send a message to the software industry about the collection of consumer data in the case of this particular enforcement action.

However, the FTC's recent enforcement activities against software companies did not end with VIZIO. In a separate statement, the **FTC announced** settlements with three other companies in the industry over allegations that they had made deceptive statements in their privacy policies about their participation in an international privacy program. The companies charged in those cases were, Sentinel Labs, Inc., a software company providing endpoint protection software to enterprise customers; SpyChatter, Inc., a company marketing a private messaging app; and Vir2us, Inc., a distributor of cybersecurity software. The FTC alleged in each complaint that the companies violated the FTC Act by making deceptive

statements about their participation in privacy programs. Attached are the complaints against **Sentinel Labs**, **SpyChatte**r, and **Vir2us**. In these cases, the proposed settlements merely prohibited the companies from making further misrepresentations about their participation in third party privacy or security programs, but are not final orders and still subject to possible amendment.

What conclusions should you as a software company take away from the FTC's recent enforcement activities against software companies? Clearly, the FTC is cognizant of the trends in the software industry to monetize data collected from software, to adopt privacy policies without actually customizing them to the practices of their particular company, and to bury privacy notices on websites without actually obtaining clear end user consent to actual business data collection practices. So, if your company is like most in this space, you are on notice that your practices need to change. Your privacy policy needs to be customized to the business practices of your particular company, which means that you actually need to take the time to consider each and every piece of information that you are collecting from the public and disclose what you are doing with it. If your customers expect you to be a part of an international privacy program before they do business with you, you need to actually take the steps requirement to receive the appropriate certification from that organization before you advise consumers and the public that you are a member. And if your software collects information, you need to make sure that not only your customers but also the parties from whom the information is collected have given their clear consent to your collection practices. A privacy policy buried in your website is probably not sufficient to cover you legally.

If you do not change your privacy practices, you are on notice that you may soon be hearing from the FTC.

Recent FTC Enforcement Actions Should Serve as a Warning to Software Industry Regarding Privacy Practices

If your company is like most and you have given little or no thought to your company's privacy policy while also collecting data and looking for ways to monetize it, then you may want to rethink how you are operating in light of recent enforcement actions by the FTC in the user data space. The Silicon Valley Software Law Blog addressed these developments in the following blogpost:

http://www.siliconvalleysoftwarelaw.com/recent-ftc-enforcement-actions-should-serve-as-warning-to-software-industry-about-privacy-practices/

Silicon Valley Software Lawyer Kristie Prinz to Speak

at Upcoming Webinar on SaaS Contracts

Prinz Law Office Press Release 3.7.2017